What is claimed is:

1. A method of secure data transmission over an unsecured network, comprising:

(a) linking a first local terminal to a server via the network;

(b) signaling to the server from the first local terminal that a secure transmission of a data document resident on the first local terminal is desired;

(c) downloading an encryption applet resident on the server into random access memory on the first local terminal;

(d) encrypting the data document using the encryption applet to create an encrypted data document on the first local terminal;

(e) uploading the encrypted data document from the first local terminal to the server via the network;

(f) linking a second local terminal to the server via the network;

(g) signaling to the server from the second local terminal that a secure transmission of the encrypted data document on the server is desired;

(h) downloading the encrypted data document from the server to the second local terminal;

(i) downloading a decryption applet resident on the server into random access memory on the second local terminal; and

(j) decrypting the encrypted data document using the decryption applet to recreate the data document on the second local terminal.

2. The method of claim 1, wherein step (a) further comprises authentication of the first local terminal; and step (g) further comprises authentication of the second local terminal.

3. The method of claim 1, wherein steps (b), (c), (d) and (e) are initiated and carried out by a single command from the first local terminal, and steps (g), (h), (i) and (j) are initiated and carried out by a single command from the second local terminal.

4. The method of claim 1, further comprising:

(k) deleting the encryption applet from the random access memory on the first local terminal; and

(l) deleting the decryption applet from the random access memory on the second local terminal.

5. The method of claim 3, wherein steps (b), (c), (d), (e) and (k) are initiated and carried out by a single command from the first local terminal, and steps (g), (h), (i), (j) and (l) are initiated and carried out by a single command from the second local terminal.

6. The method of claim 1, further comprising:

(m) downloading a hashing applet resident on the server into random access memory on the first local terminal;

(n) creating a hash of the encrypted data document using the hashing applet on the first local terminal;

(o) uploading the hash of the encrypted data document from the first local terminal to the server via the network;

(p) downloading the hash of the encrypted data document from the server to the second local terminal via the network;

(q) downloading the hashing applet resident on the server into random access memory on the second local terminal;

(r) creating a second hash of the downloaded encrypted data document using the hashing applet on the second local terminal;

(s) comparing the first hash of the encrypted data document and the second hash of the downloaded encrypted data document on the second local terminal; and

(t) displaying an error message on the second local terminal if the first hash of the encrypted data document does not match the second hash of the downloaded encrypted data document.

7. The method of claim 1, further comprising:

(u) deleting the hashing applet from the random access memory on the first local terminal; and

(v) deleting the hashing applet from the random access memory on the second local terminal.

8. The method of claim 6, further comprising:

(w) designating a keyword on the first local terminal;

(x) creating a hash of the keyword using the hashing applet on the first local terminal;

(y) encrypting the data document in step (d) using the hash of the keyword as an encryption key;

(z) creating a keyphrase as a clue to the keyword;

(aa) communicating the keyphrase to an intended recipient of the data document;

(bb) entering the keyword corresponding to the keyphrase on the second local terminal;

(cc) creating a second hash of the keyword using the hashing applet on the second local terminal;

(dd) decrypting the encrypting the data document in step (j) using the second hash of the keyword as a decryption key.

9. The method of claim 8, wherein at least one of the first and second local terminals is located in a publicly accessible location and connected to a means for recording the data document in a tangible medium.

10. The method of claim 9, wherein the means for recording the data document in a tangible medium includes a means for erasing, overwriting and/or destroying the data document on the tangible medium upon detection of an error or incomplete transaction.

11. The method of claim 1, wherein at least one of the first and second local terminals is located in a secured business location and connected to a means for recording the data document on a tangible medium.

12. The method of claim 11, further comprising delivering the data document recorded on the tangible medium from the secured business location to an intended recipient.

13. The method of claim 6, further comprising:

(w) designating a keyword on the first local terminal;

(x) combining the keyword with a public or private key to create a semi-private encryption key;

(y) creating a hash of the semi-private encryption key using the hashing applet on the first local terminal;

(z) encrypting the data document in step (d) using the hash of the semi-private encryption key as an encryption key;

(aa) creating a keyphrase as a clue to the keyword;

(bb) communicating the keyphrase to an intended recipient of the data document;

(cc) entering the keyword corresponding to the keyphrase on the second local terminal;

(dd) combining the keyword with the public or private key to recreate the semi-private encryption key;

(ee) creating a second hash of the semi-private encryption key using the hashing applet on the second local terminal;

(ff) decrypting the encrypting the data document in step (j) using the second hash of the semi-private encryption key as a decryption key.